The application/cms Media Type

Abstract

This document registers the application/cms media type for use with the corresponding CMS (Cryptographic Message Syntax) content types.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7193.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

[RFC5751] registered the application/pkc7-mime media type. That document defined five optional smime-type parameters. The smime-type parameter originally conveyed details about the security applied to the data content type, indicating whether it was signed or enveloped, as well as the name of the data content; it was later expanded to indicate whether the data content is compressed and whether the data content contained a certs-only message. This document does not affect those registrations as this document places no requirements on S/MIME (Secure Multipurpose Internet Mail Extensions) agents.

The registration done by the S/MIME documents was done assuming that there would be a MIME (Multipurpose Internet Mail Extensions) wrapping layer around each of the different enveloping contents; thus, there was no need to include more than one item in each smime-type. This is no longer the case with some of the more advanced enveloping types. Some protocols such as the CMC (Certificate Management over Cryptographic Message Syntax) [RFC5273] have defined additional S/MIME types. New protocols that intend to wrap MIME content should continue to define a smime-type string; however, new protocols that intend to wrap non-MIME types should use this mechanism instead.

CMS (Cryptographic Message Syntax) [RFC5652] associates a content type identifier (OID) with specific content; CMS content types have been widely used to define contents that can be enveloped using other CMS content types and to define enveloping content types some of which provide security services. CMS protecting content types, those that provide security services, include: Signed-Data [RFC5652], Enveloped-Data [RFC5652], Digested-Data [RFC5652], Encrypted-Data [RFC5652], Authenticated-Data [RFC5652], Authenticated-Enveloped-Data [RFC5083], and Encrypted Key Package [RFC6032]. CMS non-protecting content types, those that provide no security services but encapsulate other CMS content types, include: Content Information [RFC5652], Compressed Data [RFC3274], Content Collection [RFC4073], and Content With Attributes [RFC4073]. Then, there are the innermost content types that include: Data [RFC5652], Asymmetric Key Package [RFC5958], Symmetric Key Package [RFC6031], Firmware Package [RFC4108], Firmware Package Load Receipt [RFC4108], Firmware Package Load Error [RFC4108], Trust Anchor List [RFC5914], TAMP Status Query, TAMP Status Response, TAMP Update, TAMP Update Confirm, TAMP Apex Update, TAMP Apex Update Confirmation, TAMP Community Update, TAMP Community Update Confirm, TAMP Sequence Adjust, TAMP Sequence Adjust Confirmation, TAMP Error [RFC5934], Key Package Error, and Key Package Receipt [RFC7191].
To support conveying CMS content types, this document defines a media type and parameters that indicate the enveloping and embedded CMS content types.

New CMS content types should be affirmative in defining the string that identifies the new content type and should additionally define if the new content type is expected to appear in the encapsulatedContent or innerContent parameter.

1.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. CMS Media Type Registration Applications

This section provides the media type registration application for the application/cms media type (see [RFC6838], Section 5.6).

Type name: application

Subtype name: cms

Required parameters: None.

Optional parameters:

encapsulatingContent=y; where y is one or more CMS ECT (Encapsulating Content Type) identifiers; multiple values are encapsulated in quotes and separated by a folding-whitespace, a comma, and folding-whitespace. ECT values are based on content types found in [RFC3274], [RFC4073], [RFC5083], [RFC5652], and [RFC6032]. This list can later be extended; see Section 4.
innerContent=x; where x is one or more CMS ICT (Inner Content Type) identifiers; multiple values encapsulated in quotes and are separated by a folding-whitespace, a comma, and folding-whitespace. ICT values are based on content types found in [RFC4108], [RFC5914], [RFC5934], [RFC5958], [RFC6031], and [RFC7191]. This list can later be extended; see Section 4.

firmwarePackage
firmwareLoadReceipt
firmwareLoadError
aKeyPackage
sKeyPackage
trustAnchorList
TAMP-statusQuery
TAMP-statusResponse
TAMP-update
TAMP-updateConfirm
TAMP-apexUpdate
TAMP-apexUpdateConfirm
TAMP-communityUpdate
TAMP-communityUpdateConfirm
TAMP-seqNumAdjust
TAMP-seqNumAdjustConfirm
TAMP-error
keyPackageReceipt
keyPackageError

The optional parameters are case sensitive.

Encoding considerations:

Binary.

[RFC5652] requires that the outermost encapsulation be ContentInfo.
Security considerations:

The following security considerations apply:

<table>
<thead>
<tr>
<th>RFC</th>
<th>CMS Protecting Content Type and Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td>[RFC3370]</td>
<td>signedData, envelopedData,</td>
</tr>
<tr>
<td>[RFC5652]</td>
<td>digestedData, encryptedData, and</td>
</tr>
<tr>
<td>[RFC5753]</td>
<td>authData</td>
</tr>
<tr>
<td>[RFC5754]</td>
<td></td>
</tr>
<tr>
<td>[RFC5958]</td>
<td>aKeyPackage</td>
</tr>
<tr>
<td>[RFC5959]</td>
<td></td>
</tr>
<tr>
<td>[RFC6162]</td>
<td></td>
</tr>
<tr>
<td>[RFC6031]</td>
<td>sKeyPackage</td>
</tr>
<tr>
<td>[RFC6160]</td>
<td></td>
</tr>
<tr>
<td>[RFC6032]</td>
<td>encryptedKeyPkg</td>
</tr>
<tr>
<td>[RFC6033]</td>
<td></td>
</tr>
<tr>
<td>[RFC6161]</td>
<td></td>
</tr>
<tr>
<td>[RFC5914]</td>
<td>trustAnchorList</td>
</tr>
<tr>
<td>[RFC3274]</td>
<td>compressedData</td>
</tr>
<tr>
<td>[RFC5083]</td>
<td>authEnvelopedData</td>
</tr>
<tr>
<td>[RFC5084]</td>
<td></td>
</tr>
<tr>
<td>[RFC4073]</td>
<td>contentCollection and contentWithAttrs</td>
</tr>
<tr>
<td>[RFC4108]</td>
<td>firmwarePackage, firmwareLoadReceipt, and firmwareLoadError</td>
</tr>
<tr>
<td>[RFC5934]</td>
<td>TAMP-statusQuery, TAMP-statusResponse, TAMP-update, TAMP-updateConfirm,</td>
</tr>
<tr>
<td></td>
<td>TAMP-apexUpdate, TAMP-apexUpdateConfirm, TAMP-communityUpdate,</td>
</tr>
<tr>
<td></td>
<td>TAMP-communityUpdateConfirm, TAMP-seqNumAdjust, TAMP-seqNumAdjustConfirm, and</td>
</tr>
<tr>
<td></td>
<td>TAMP-error</td>
</tr>
<tr>
<td>[RFC7191]</td>
<td>keyPackageReceipt and keyPackageError</td>
</tr>
</tbody>
</table>

---

In some circumstances, significant information can be leaked by disclosing what the innermost ASN.1 structure is. In these cases, it is acceptable to disclose the wrappers without disclosing the inner content type.

ASN.1 encoding rules (e.g., DER and BER) have a type-length-value structure, and it is easy to construct malicious content with invalid length fields that can cause buffer overrun conditions. ASN.1 encoding rules allows for arbitrary levels of nesting, which may make it possible to construct malicious content that will cause a stack overflow. Interpreters of ASN.1 structures should be aware of these issues and should take appropriate measures to guard against buffer overflows and stack overruns in particular and malicious content in general.

Interoperability considerations:

See [RFC3274], [RFC4073], [RFC4108], [RFC5083], [RFC5652], [RFC5914], [RFC5934], [RFC5958], [RFC6031], [RFC6032], and [RFC7191].

In all cases, CMS content types are encapsulated within ContentInfo structures [RFC5652]; that is the outermost enveloping structure is ContentInfo.

CMS [RFC5652] defines slightly different processing rules for SignedData than does PKCS #7 [RFC2315]. This media type employs the CMS processing rules.

The Content-Type header field of all application/cms objects SHOULD include the optional "encapsulatingContent" and "innerContent" parameters.

The Content-Disposition header field [RFC4021] can also be included along with Content-Type’s optional name parameter.

Published specification: This specification.

Applications that use this media type:

Applications that support CMS (Cryptographic Message Syntax) content types.

Fragment identifier considerations: N/A
Additional information:

   Magic number(s): None
   File extension(s): .cmsc
   Macintosh File Type Code(s):

Person & email address to contact for further information:

   Sean Turner <turners@ieca.com>

Intended usage: COMMON

Restrictions on usage: none

Author: Sean Turner <turners@ieca.com>

Change controller: The IESG <iesg@ietf.org>
3. Example

The following is an example encrypted status response message:

```
MIME-Version: 1.0
Content-Type: application/cms; encapsulatingContent=encryptedData;
            innerContent=TAMP-statusResponse; name=status.cmsc
Content-Transfer-Encoding: base64
```

Base64-encoded content:

```
MIIFLQYJKoZ2IhvcNAQcDOIFIHjcCBBROCAxgBgMiIBQIBADBFBMEAcX
zAJBgNVAYYtaelingIENCBQYmqCxAqGAMG0GCSqGSIb3DQEBAQUA
uaXQeVsoY7z7giz0PjikRQ6fJq64k2dbHEB45DZL/ueRF9FUIja9La
5387E7w3fOMDUaDhGfQVrKOPrNTsLmww8fE/O+wcqP2I2XaILOR62D
emQqSt+EPFMw2ZG9q0mmY3AxeFagzprhV8gK75DiGXFq89ux9PmdC
5jhpIgcAUFHn6Iq7yd72O1087LCM1Xm3g5rSyUggxoceFHNiPNR28TV5
HctG
```

4. IANA Considerations

IANA has registered the media type application/cms in the Standards tree using the applications provided in Section 2 of this document.
IANA has established two subtype registries called "CMS Encapsulating Content Types" and "CMS Inner Content Types". Entries in these registries are allocated by Expert Review \[RFC5226\]. The Expert will determine whether the content is an ECT or an ICT, where the rule is that an ICT does not encapsulate another content type while an ECT does encapsulate another content type.

Initial values are as follows:

### CMS Encapsulating Content Types

<table>
<thead>
<tr>
<th>Name</th>
<th>Document</th>
<th>Object Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>authData</td>
<td>[RFC5652]</td>
<td>1.2.840.113549.1.9.16.1.2</td>
</tr>
<tr>
<td>compressedData</td>
<td>[RFC3274]</td>
<td>1.2.840.113549.1.9.16.1.9</td>
</tr>
<tr>
<td>contentCollection</td>
<td>[RFC4073]</td>
<td>1.2.840.113549.1.9.16.1.19</td>
</tr>
<tr>
<td>contentInfo</td>
<td>[RFC5652]</td>
<td>1.2.840.113549.1.9.16.1.6</td>
</tr>
<tr>
<td>contentWithAttrs</td>
<td>[RFC4073]</td>
<td>1.2.840.113549.1.9.16.1.20</td>
</tr>
<tr>
<td>authEnvelopedData</td>
<td>[RFC5083]</td>
<td>1.2.840.113549.1.9.16.1.23</td>
</tr>
<tr>
<td>encryptedKeyPkg</td>
<td>[RFC6032]</td>
<td>2.16.840.1.101.2.1.2.78.2</td>
</tr>
<tr>
<td>digestData</td>
<td>[RFC5652]</td>
<td>1.2.840.113549.1.9.16.1.5</td>
</tr>
<tr>
<td>encryptedData</td>
<td>[RFC5652]</td>
<td>1.2.840.113549.1.9.16.1.6</td>
</tr>
<tr>
<td>envelopedData</td>
<td>[RFC5652]</td>
<td>1.2.840.113549.1.9.16.1.12</td>
</tr>
<tr>
<td>signedData</td>
<td>[RFC5652]</td>
<td>1.2.840.113549.1.9.16.1.13</td>
</tr>
</tbody>
</table>

### CMS Inner Content Types

<table>
<thead>
<tr>
<th>Name</th>
<th>Document</th>
<th>Object Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>firmwarePackage</td>
<td>[RFC4108]</td>
<td>1.2.840.113549.1.9.16.1.16</td>
</tr>
<tr>
<td>firmwareLoadReceipt</td>
<td>[RFC4108]</td>
<td>1.2.840.113549.1.9.16.1.17</td>
</tr>
<tr>
<td>firmwareLoadError</td>
<td>[RFC4108]</td>
<td>1.2.840.113549.1.9.16.1.18</td>
</tr>
<tr>
<td>aKeyPackage</td>
<td>[RFC5958]</td>
<td>2.16.840.1.101.2.1.2.78.5</td>
</tr>
<tr>
<td>sKeyPackage</td>
<td>[RFC6031]</td>
<td>1.2.840.113549.1.9.16.1.25</td>
</tr>
<tr>
<td>trustAnchorList</td>
<td>[RFC5914]</td>
<td>1.2.840.113549.1.9.16.1.34</td>
</tr>
<tr>
<td>TAMP-statusQuery</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.1</td>
</tr>
<tr>
<td>TAMP-statusResponse</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.2</td>
</tr>
<tr>
<td>TAMP-update</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.3</td>
</tr>
<tr>
<td>TAMP-updateConfirm</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.4</td>
</tr>
<tr>
<td>TAMP-apexUpdate</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.5</td>
</tr>
<tr>
<td>TAMP-apexUpdateConfirm</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.6</td>
</tr>
<tr>
<td>TAMP-communityUpdate</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.7</td>
</tr>
<tr>
<td>TAMP-communityUpdateConfirm</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.8</td>
</tr>
<tr>
<td>TAMP-seqNumAdjust</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.9</td>
</tr>
<tr>
<td>TAMP-seqNumAdjustConfirm</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.11</td>
</tr>
<tr>
<td>TAMP-error</td>
<td>[RFC5934]</td>
<td>2.16.840.1.101.2.1.2.77.7</td>
</tr>
<tr>
<td>keyPackageReceipt</td>
<td>[RFC7191]</td>
<td>2.16.840.1.101.2.1.2.78.3</td>
</tr>
<tr>
<td>keyPackageError</td>
<td>[RFC7191]</td>
<td>2.16.840.1.101.2.1.2.78.6</td>
</tr>
</tbody>
</table>
5. Security Considerations

See the answer to the Security Considerations template questions in Section 2.

6. Acknowledgments

Special thanks to Carl Wallace for generating the example in Section 3.

7. References

7.1. Normative References


7.2. Informative References


Authors’ Addresses

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com
Phone: +1.703.628.3180

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com

Jim Schaad
Soaring Hawk Consulting

EMail: ietf@augustcellars.com